

Coronavirus texting scams: 5 ways to protect yourself on your phone

Jason Cipriani At CNET

Don't answer texts claiming to have a cure for COVID-19, or offering test kits. It's a scam.

Scammers and spammers are already feeding off public fears of the coronavirus pandemic to scare people into turning over sensitive personal information and money. Working from home puts people at greater risk from hackers trying to take advantage of an unsettling global situation. Calls and texts offering potential treatments or test kits or claiming to be from the Social Security Administration are on the rise. As one example, this week Android Police contributor Corbin Davenport received an obvious spoof text message from someone posing as his bank.

The Federal Communications Commission has outlined some of the COVID-19 scams it's identified, and the Federal Trade Commission also has a list of common scams that have been reported. Even the FBI has issued a warning for COVID-19 stimulus package scams.

COVID-19-related messages are only one type of text scam; for example, scammers also send out messages claiming your iCloud account has been hacked in a bid to trick you into handing over your account information. Armed with that information, they can then use it to take over your phone number or access your online accounts.

Below are some general tips on what to do -- and what *not* to do -- when you receive a spam text.

Don't open any links

Scammers are tricky. They'll send messages that appear to be from a legitimate company, such as your wireless carrier, bank or medical facility, and include a link asking you to verify your account information. The link then takes you to a site that may look real, but is actually fake. The object is to collect your username, password and other personal information for future use.

If you receive an unexpected message that includes a link, do not open it. If you happen to open it, do not enter any account details or personal information.

Look at this fake Verizon site that was being used in phishing attempts, as covered by How To Geek. The site looks real and even redirects to the official Verizon site after the nefarious actors have taken your account credentials. Scary stuff.

Coronavirus texting scams: 5 ways to protect yourself on your phone

Do research before replying with STOP

One common method of opting out of receiving non-nefarious spam texts (like that restaurant offering the free milkshake) is to reply to the message with "STOP." It can be a quick and easy way to end messages from everything from a political campaign to your internet service provider.

But scammers use this same tool to trick you into replying to their messages, in turn letting them know that your phone number is valid and one they can target with more messages or robocalls.

Instead of quickly replying STOP to an unsolicited message, take a few seconds to look up the number online to see if a recognized organization or business uses it for text messages.

I verified Comcast's number, for example, by searching for "text from 266278" after receiving a message a few weeks ago asking if I wanted updates about an outage in my area. Indeed, the number I received the message from matched a number Comcast lists on its support page.

If you verify that a number is valid, reply with STOP to remove yourself from their distribution list.

Report a bad message to your carrier

If you can't verify who sent a message, or it's clearly a scam, you can forward the message to 7726 (it spells "spam" on a phone's keypad).

AT&T, Sprint, T-Mobile and Verizon all accept spam reports through this number. You may receive a follow-up message after reporting a message, asking for more information or to confirm the number the original message was sent from.

Some carriers, such as Sprint, will even block the number from messaging you after you've reported it.

Use your phone's built-in blocking tool

Another option is to block the number yourself. Both iOS and Android have built-in tools to block messages and calls from specific numbers.

Coronavirus texting scams: 5 ways to protect yourself on your phone

iPhone users

On an iPhone, open the message in the Messages app and tap on the profile photo at the top, then tap on the **Info** button. On the next screen, tap on the **phone number** followed by **Block this Caller** at the bottom of the next screen.

Following those steps will block the number from both messaging and calling you.

Android users

As is usually the case with Android phones, the process to block a number will vary depending on who makes your phone and which message app you're using.

If you're using Google's Messages app, start by opening the spam message, then tapping on the menu button in the top-right corner and selecting **Details** from the list of options. On the following screen, select **Block & report spam** followed by **OK**. The Messages app will send the number and the 10 previous messages from it to Google for analysis to improve future spam detection. Your replies to the number are not sent to Google. If you'd rather just block the number, uncheck the box next to "Report spam" before tapping **OK**.

Samsung Messages users will need to open the conversation, tap on the three-dot menu in the top-right corner and select **Block number** > **Block**.

File a complaint with the FCC

If you want to help combat current and future spam messages, and you're in the US, you can file a complaint with the Federal Communications Commission whenever you receive a message that falls into one of these three categories:

- An unsolicited commercial text message
- An automated message sent to your phone without your prior consent
- An automated message from a telecommunications company, or another company advertising a telecommunications company's products or services sent without your prior consent

Visit this site to file a complaint with the FCC. It won't immediately stop messages from arriving on your phone, but it will at least help the FCC track down bad actors.

Just as you don't have to deal with spam messages, you don't have to deal with robocalls either. You won't be able to put an end to them for good, but you can at least cut back on the number of times your phone rings. And remember, there are plenty of red flags when it comes to coronavirus scams, so make sure you know them

Coronavirus texting scams: 5 ways to protect yourself on your phone

all. While you're at it, take a few minutes to [secure your wireless account to prevent SIM swap fraud](#).